

CITY AUDITOR'S OFFICE



AUDIT OF INFORMATION TECHNOLOGY SECURITY

Report CAO 2101-0102-09

June 13, 2002

**RADFORD K. SNELDING, CPA, CIA, CFE
CITY AUDITOR**



June 13, 2002

MAYOR
OSCAR B. GOODMAN

CITY COUNCIL
GARY REESE
(MAYOR PRO-TEM)
MICHAEL J. McDONALD
LARRY BROWN
LYNETTE B. McDONALD
LAWRENCE WEEKLY
MICHAEL MACK

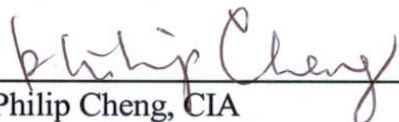
CITY MANAGER
VIRGINIA VALENTINE


Mayor Oscar B. Goodman
Councilman Gary Reese (Mayor Pro-Tem)
Councilman Michael J. McDonald
Councilman Larry Brown
Councilwoman Lynette Boggs McDonald
Councilman Lawrence Weekly
Councilman Michael Mack
City of Las Vegas Audit Committee


Subject: CAO 2101-0102-09 - Audit of Information Technology Security

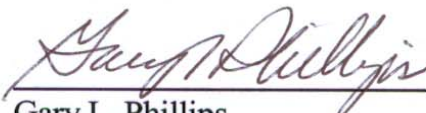
Attached please find the report mentioned above. Management comments are included following the report.

Prepared by:


Philip Cheng, CIA
Sr. Internal Auditor


William C. Cimo, CISA
Sr. Information Technology Auditor

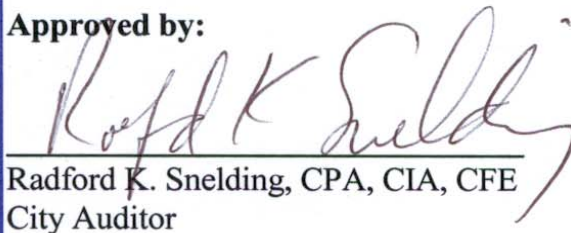

Bryan L. Smith, CPA
Internal Auditor


Gary L. Phillips
Internal Auditor

CITY AUDITOR'S OFFICE

CITY AUDITOR
RADFORD K. SNELDING
CIA, CPA, CFE

Approved by:


Radford K. Snelding, CPA, CIA, CFE
City Auditor

CITY OF LAS VEGAS
400 STEWART AVENUE
LAS VEGAS, NEVADA 89101

VOICE 702.229.2472

FAX 702.386.9252

TDD 702.386.9108

www.ci.las-vegas.nv.us

TABLE OF CONTENTS

BACKGROUND	1
OBJECTIVES	1
SCOPE AND METHODOLOGY	1
FINDINGS AND RECOMMENDATIONS	2
1. RISK ANALYSIS	2
2. INFORMATION TECHNOLOGY SECURITY TRAINING	3
3. INCIDENT AND INTRUSION MONITORING, DETECTION, HANDLING, REPORTING, AND LOGGING	3
4. PENETRATION TESTING	5
5. SOCIAL ENGINEERING	5
6. PATCHES	6
7. WIRELESS SECURITY	7
8. SYSTEM ACCESS AND AUTHENTICATION	8
9. DOMAIN ADMINISTRATOR RIGHTS	9
10. ROOT ACCESS	9
11. LOCAL ADMINISTRATOR	10
12. CONTROL OF COMPUTERS AND EQUIPMENT	10
13. LONG DISTANCE CODES	11
14. SECURITY COMMITTEE	12
15. MULTIPLE SESSIONS	12
16. COMPUTER ROOM LOCATION	13
17. EMPLOYEE TERMINATION PROCEDURES	14
MANAGEMENT RESPONSES	14

AUDIT OF INFORMATION TECHNOLOGY SECURITY

REPORT CAO 0201-0102-09

BACKGROUND

Information Technology Security (IT Security) is protecting and preserving systems and data from unauthorized manipulation or viewing. IT Security includes concepts, techniques, technical measures, and administrative policies and procedures used to protect information assets from deliberate or inadvertent unauthorized access, acquisition, damage, disclosure, manipulation, modification, loss, or use. A basic tenet of security is that it is only as strong as its weakest link.

The City's IT Department has an Information Security and Contingency Administrator who provides technical development and administration for logical and physical information security. IT Security is critical because of the essential services the City provides such as business licensing, sewer services, and wastewater treatment and the impact on revenue and customer service. Additionally, IT Security is important in protecting the different methods of access such as wireless, dial-in, or accessing the systems from remote locations. Finally, IT Security helps in unforeseen situations, such as the September 11th tragedy because you never know when or where a system will be targeted.

Information Technologies' budget for expenditures was \$10.59 million for fiscal year 2001. The City owns approximately 4,800 pieces of microcomputer and peripheral equipment with a cost of approximately \$4.76 million. The City has approximately 2,500 employees with computer access to city systems.

OBJECTIVES

We have completed an audit of IT Security. This audit was part of the City Auditor's Office annual audit plan. Our objectives included the following:

- Determine whether city assets and data are safeguarded from loss;
- Review and evaluate efficiency, effectiveness, and adequacy of operational, financial, and system controls; and
- Review compliance with policies and procedures.

SCOPE AND METHODOLOGY

Our audit was performed in accordance with generally accepted governmental auditing standards. We evaluated the efficiency and effectiveness of the City's IT Security. Audit

procedures included:

- Reviewing policies and procedures;
- Reviewing the City Charter;
- Interviewing staff and management;
- Observing operations;
- Analyzing operational data; and
- Evaluating security and access controls.

FINDINGS AND RECOMMENDATIONS

The following issues were identified during the audit. While other issues were identified and discussed with management, they were deemed less significant for reporting purposes.

1. RISK ANALYSIS

Criteria:

- Risk Analysis should be properly acknowledged and dated.

Condition:

- In 1997, the City's Information Security & Contingency Administrator prepared the *Risk Analysis for the City of Las Vegas (CLV) Information Technologies Department* (Risk Analysis). This document identifies and analyzes threats that have the potential of interrupting information processing or destroying information resources and systems.
- The last page of the Risk Analysis includes the following statement and signature lines for the IT Director and the Deputy City Manager: "I have reviewed and approved this Risk Assessment. I will ensure recommended countermeasures be implemented, provide acceptable alternative measures or accept the potential vulnerabilities."
- While the Risk Analysis is included on the City's intranet for access by employees, this document was never acknowledged or signed by the IT Director, a Deputy City Manager, or the City Manager. In addition, the document is not dated.
- According to the Information Security & Contingency Administrator, the Risk Analysis is updated periodically as circumstances change, however changes to the document could not be identified.
- No management action plans in response to the recommendations within the Risk Analysis are identified.

Cause:

- Objective of Risk Analysis not clearly defined.

Effect:

- Lack of accountability for taking action on identified threats.
- Lack of formal approval to carry out recommendations identified in document.
- Status of actions taken in response to Risk Analysis is unclear.

Recommendations:

1. The Director of Information Technology should evaluate the Risk Analysis and determine whether to acknowledge it as a formal document. If reviewed and acknowledged, IT Management should sign and date the document and create an action plan in response to the recommendations within the document.
2. The Risk Analysis and management action plan should be forwarded to the City Manager's Office for review and acknowledgement.
3. Revisions to the original Risk Analysis should be formally tracked.

2. INFORMATION TECHNOLOGY SECURITY TRAINING

Criteria:

- Good information technology security programs include ongoing training to employees on security policies and procedures, ownership responsibilities, and virus protection.

Condition:

- Little formal training exists for city employees on information security policies, procedures, and practices.

Cause:

- Human Resources include limited information technology security training in the new employee orientation.
- IT has not provided ongoing education related to information security issues.

Effect:

- Users may not be aware of their responsibilities related to information security.
- Increased administration time and expenditures.

Recommendation:

1. The IT Security and Contingency Administrator should work with Human Resources to develop and implement ongoing information security training programs as a way to provide new and current employees with an understanding of information security policies and procedures. This program could require users to identify through their signature that they have read and understand current policies or to pass a general information security test before obtaining access to City systems.

3. INCIDENT AND INTRUSION MONITORING, DETECTION, HANDLING, REPORTING, AND LOGGING

Criteria:

- Security controls should include the use of intrusion detection software, a methodology for reviewing incidents and logs, reporting of incidents, and timely corrective action.

Condition:

- IT does not use intrusion detection software but they are evaluating purchasing some.
- IT does not have a formal methodology for reviewing incidents, auditing, or system logs.
- IT does not document incidents.
- An incident reporting document exists on the Security Committee's intranet website but the process for using the document is not clearly outlined.
- Limited system auditing logs are enabled by IT.
- The limited system auditing logs currently enabled are only informally reviewed by the System Administrators. There is no evidence of review of system auditing logs.
- Formal assignments for review of system auditing logs have not been made.
- No system auditing / log monitoring tools are in use.
- Event logs are maintained online based on disk space allocated.
- System auditing is not maintained due to disk space requirements.
- Logs are not maintained for UNIX systems.

Cause:

- Lack of formal processes and procedures for incident reporting.
- Data storage limitations.
- Lack of a formal system auditing program.

Effect:

- Insufficient monitoring of certain system operations.
- Duplication of efforts in monitoring current system auditing logs.
- Lack of accountability of personnel for reviewing logs.

Recommendations:

1. IT Management and the Security and Contingency Administrator should:
 - ▶ Formalize the incident handling process;
 - ▶ Establish incident management responsibilities and procedures to ensure appropriate, effective, and orderly response to security incidents;
 - ▶ Establish a computer security incident handling response team to address security incidents by providing a centralized platform with sufficient expertise;
 - ▶ Review the current incident handling process for security concerns as they arise in the City's systems; and
 - ▶ Communicate the incident reporting process to city employees.
2. IT Management should identify, evaluate, and document:
 - ▶ Key system auditing/logs that should be enabled, monitored, and reviewed for discrepancies on a regular basis;
 - ▶ System auditing tools that could be used to increase monitoring of systems; and
 - ▶ A formal system monitoring program including assignment of responsibility for reviewing system auditing/logs and identification of frequency of review of logs.

4. PENETRATION TESTING

Criteria:

- Regular penetration testing increases security, closes security loopholes of known vulnerabilities, and reduces the risk and enticement of a system attack if the results of the penetration test are reviewed and appropriate system or policy changes are made.

Condition:

- IT is not performing penetration tests but they are in the process of hiring a consultant to perform some penetration tests.

Cause:

- Performing penetration tests to identify system security weaknesses has been reduced in priority for IT because of other priorities.

Effect:

- Without penetration tests, IT may not be aware of existing system weaknesses.

Recommendation:

1. IT should perform and document penetration tests on a regular basis.

5. SOCIAL ENGINEERING

Criteria:

- Social engineering (the process by which a person is tricked into revealing their system password or having someone else's password reset) can be used to obtain passwords and system access.
- Preventing social engineering should be considered when implementing new policies and procedures for IT staff.

Condition:

- Audit tested the practices of the IT Support Desk and had a password inappropriately reset. IT Support Desk staff did not adhere to the policy posted on the intranet of requiring an email from a supervisor for a password to be reset. IT Support Desk emailed the reset password to the person attempting to access another person's system without confirming their identity.
- IT uses a standard password for password resets.
- IT has established a 15 minute lockout after three unsuccessful logon attempts. The count is reset after five minutes thereby allowing the user to make more than three attempts in 15 minutes.
- Password reset procedures are not consistent for the PC and the mainframe.
- Unauthorized logon attempts can be made without IT awareness.

Cause:

- IT support desk did not follow existing policy.
- IT does not have an employee verification process in place.
- IT does not necessarily know if a user is locked out since the system allows users to logon after 15 minutes.
- Lockout does not have to be cleared by IT.

Effect:

- Unauthorized access to systems.

Recommendations:

1. IT should develop a process to verify an employee's identity before resetting a password such as questioning employees about their birthday, social security number, or other personal information or having employees physically present themselves to the IT Support Desk with identification.
2. IT should ensure that emailed passwords are only sent to supervisors.
3. After three failed logon attempts, IT should lockout users until unlocked by IT.

6. PATCHES

Criteria:

- Patches (modifications to a computer program to repair known vulnerable areas of a system that can increase security threats if appropriate actions are not taken timely to fix them) should be reviewed, assessed, and implemented as necessary through a formal process.

Condition:

- A manual log is being kept to record utilized/applied patches.
- No formal written procedures exist for tracking, evaluating, and addressing patches.
- Responsibility for tracking and evaluating patches has not been formally assigned.

Cause:

- Work activities have not been formally prioritized.

Effect:

- Potential loss of data and revenues.
- Potential negative impact on productivity, customer services, and systems.
- Increased costs.

Recommendation:

1. IT Management should establish written policy and procedures regarding patches including the following:
 - ▶ Who is responsible for identifying and tracking applicable patches;
 - ▶ How can applicable patches be identified;
 - ▶ When should patches be evaluated;
 - ▶ What criteria should be used to evaluate each patch; and

- ▶ Which patches should be applied?

7. WIRELESS SECURITY

Criteria:

- Wireless access to systems has known security vulnerabilities that should be evaluated and addressed.

Condition:

- IT is planning ten access points for wireless access, four of which have been implemented.
- While only four users have wireless access now, IT anticipates this to increase dramatically in the future.
- WEP (Wired Equivalency Protocol) has not been implemented. WEP is a security protocol that is designed to provide a wireless local area network with a level of security and privacy comparable to what is usually expected of a wired LAN (local area network).
- Administration of bridges is available via the intranet and not secured with passwords.
- Wireless access can currently be achieved without authenticating to system.

Cause:

- Factors such as time and convenience appear to be a higher priority than security during system implementations.

Effect:

- Security vulnerabilities exist and could potentially be exploited.

Recommendations:

1. IT should document, evaluate, and implement:
 - ▶ WEP;
 - ▶ MAC (Media Access Control) address authentication as an additional level of authentication;
 - ▶ A VPN (Virtual Private Network) to tunnel data over the wireless network; and
 - ▶ A client based personal firewall and intrusion detection software to alert the user and stop client to client attacks.
2. Access points should be tied into a firewall thus making each access point a DMZ (demilitarized zone) - a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. This prevents outside users from getting direct access to a company's internal network.
3. Administration of bridges should be secured via passwords.

8. SYSTEM ACCESS AND AUTHENTICATION

Criteria:

- Proper password and access controls reduce the risk of unauthorized access to systems.

Condition:

- Passwords are used by the City to restrict unauthorized access to computer systems and applications. Currently, the only restriction for user passwords is that they must be at least five characters long. Using password cracking software readily available to the public, IT identified the passwords of 1,082 of 2,213 (49%) city system users and 110 of 360 (31%) Remote Access Server (RAS) users. Enhanced system security exists with the use of longer passwords with a combination of upper case and lower case letters, numbers and special characters.
- A significant city application does not require users to periodically change their access passwords.
- The City has a local and a toll-free remote access phone number used by both employees and vendors to access city systems and applications. These phone numbers have never been changed.
- IT was in the process of implementing password hardening.

Cause:

- Insufficient evaluation of access and authentication controls.
- Many users are not following proper password protocols.
- Additional programming is needed to force users to change passwords for some applications.

Effect:

- Potential of unauthorized access to city systems and data.

Recommendations:

1. IT should improve password protocol by requiring the use of both alpha and numeric characters in passwords.
2. IT should perform systematic evaluations of user passwords to ensure that users are in compliance with password protocol. Users should be required to change their password if it does not conform to the password protocol.
3. IT should require that user passwords for all significant applications be periodically changed.
4. IT should evaluate and document how biometrics could potentially be used by the City to improve system security and the cost/benefits of implementation.
5. Remote access phone numbers should be changed annually.
6. IT should restrict the hours of access to the city network, where feasible. For example, hours of usage could be restricted during weekends and between 8 pm and 5 am for the majority of employees. Justification should be required for those requesting extending hours.

9. DOMAIN ADMINISTRATOR RIGHTS

Criteria:

- Domain Administrator Rights are the highest level of access available on an NT Server. These rights are typically reserved for system administrators. As the number of individuals with these rights increases, the risk exposure to the system increases.

Condition:

- In addition to the three system administrators, the Microcomputer Support Supervisor and a Computer Systems Technician have Domain Administrator Rights to the City's NT Server.
- Methods exist by which a subset of Domain Administrator Rights could be granted to an individual, further restricting the number of individuals with Domain Administrator Rights.

Cause:

- Alternative methods to give limited access to Domain Administrator Rights have not been adequately evaluated.

Effect:

- Increased risk exposure to city systems.

Recommendation:

1. IT Management should evaluate methods by which a subset of Domain Administrator Rights can be granted to non-system administrator employees with such a need to perform their job.

10. ROOT ACCESS

Criteria:

- Root access to the UNIX system is the privileged system maintenance login for almost unlimited access to the system. Root access to the UNIX system must be properly controlled. The number of users with root access should be limited and the password should be changed regularly to protect the system.

Condition:

- The City currently has ten users with root access including seven operations staff and three system administrators.
- No documented criteria exists outlining who should have root access.
- The root access password is only changed at most once a year.

Cause:

- Inadequate evaluation of security risks related to root access.

Effect:

- Increased risk of unauthorized access to the UNIX system.

Recommendations:

1. IT Management should develop and document a policy outlining what positions should have root access and make changes as necessary to the access of those who currently have root access.
2. The root access password should be changed more frequently (for example, every 90 days).

11. LOCAL ADMINISTRATOR

Criteria:

- A local administrator ID (identification) is an ID with administrative rights over a PC (personal computer) and changes made to the PC locally.
- Administrator IDs should be renamed to increase system security.

Condition:

- All city computers have a local administrator account named “administrator”.
- IT has not renamed the local administrator accounts.
- IT uses the same password for all local administrator accounts.

Cause:

- IT does not rename standard IDs such as “administrator”.

Effect:

- By using the same ID for local administrator accounts, a user who is able to crack the password for one local administrator account will have access to all systems with a local administrator account.

Recommendations:

1. IT should rename local administrator accounts.
2. IT should have different passwords for local administrator accounts.

12. CONTROL OF COMPUTERS AND EQUIPMENT

Criteria:

- Proper internal control of assets includes accurate and timely physical inventories. Additionally, the location of assets and their condition should be tracked.

Condition:

- The City owns approximately 4,800 pieces of computer equipment costing approximately \$4.76 million.
- The City has approximately 2,500 employees with computer access.
- A physical inventory of these computers and equipment was completed by IT on October 31, 2001. This inventory included the placement of bar code labels on the computers and equipment. This process was overseen by the Microcomputer Support Supervisor and was very time and labor intensive.

- IT currently plans on completing a physical inventory of computers and equipment every three years using recently acquired scanners and software.
- No formal physical inventory procedures have been created.
- City employees agree to abide by the *Use of City of Las Vegas IT Resources* document when they are granted access to the City's systems. This document does not outline the responsibilities of users for proper care and security of computers and equipment or identify the repercussions of abuse or damage of computers and equipment.
- City employees are not held accountable for abuse to city computers and equipment.

Cause:

- Inadequate inventory control procedures.
- Incomplete policies.

Effect:

- Theft and damage of computers and equipment may not be timely identified with a physical inventory only being completed every three years.
- Lack of personal accountability by employees.

Recommendations:

1. IT should conduct cyclical physical inventories of computers and equipment annually with the involvement of city departments. In conjunction with these inventories, explanations for unaccounted for or damaged property should be obtained and appropriate action taken.
2. IT should create written physical inventory procedures.
3. The *Use of City of Las Vegas IT Resources* document should be updated to include the responsibilities of users for proper care and security of computers and equipment and the repercussions of abuse or damage to this property.
4. IT should develop a policy that holds city employees monetarily accountable for verifiable abuse of city computers and equipment. Once such a policy has been developed, a program to enforce this policy should be implemented.

13. LONG DISTANCE CODES

Criteria:

- Codes (passwords) should be of a nature that they are not easily guessed.

Condition:

- There are approximately 5,000 activated five digit long distance codes assigned to the City by Sprint. Approximately 2,000 of these codes are currently assigned to employees. With five digits, there are 100,000 possible combinations and with 5,000 activated codes then one out of every 20 combinations is a valid code.
- Audit was able to successfully guess two activated long distance codes in a few minutes.
- By increasing the long distance codes to six digits, there would be 1,000,000 combinations, and only having assigned codes be activated (approximately 2,000), then only one out of every 500 combinations would be a valid code and the opportunity for guessing a code would be greatly reduced.

- Phone codes have not been changed for users since the five digit codes were introduced a few years ago.

Cause:

- IT has phone codes activated that are not assigned to employees.

Effect:

- By having more codes activated than necessary, the risk of phone codes being misused is increased.

Recommendations:

1. Long distance codes that are not assigned to an employee should not be activated.
2. Long distance codes should be increased in length to improve security.
3. Long distance codes should be changed on a regular basis.

14. SECURITY COMMITTEE

Criteria:

- An effective security committee is actively involved in formulating strategies and promoting awareness of security related issues.

Condition:

- The City's Security Committee has been established for many years.
- Most employees including the system administrators are not aware of the existence of the Security Committee.
- Currently, the Security Committee only addresses physical security related issues. The Configuration Control Committee currently handles system security issues. Roles and responsibilities of these committees are not clearly defined.

Cause:

- IT Management and the City Marshal's Office have not clearly defined the roles and responsibilities of the Security Committee.

Effect:

- Critical IT security issues could be overlooked.

Recommendations:

1. IT Management should clearly define the roles and responsibilities of the Security Committee to ensure all IT security issues are being addressed in a timely manner.
2. IT Management should review, document, and implement a methodology to ensure that IT security issues are reviewed and addressed by a committee.

15. MULTIPLE SESSIONS

Criteria:

- Simultaneous access to multiple computers (multiple sessions) creates increased exposure to unauthorized access to a system.

Condition:

- City employees can simultaneously log onto an unlimited number of computers at once.
- IT has the capability of assigning users access to particular workstations.

Cause:

- IT permits this practice for the convenience of users.

Effect:

- Increased exposure to unauthorized access of city systems.

Recommendation:

1. IT should restrict access of users, where feasible, to a single computer workstation. Special authorization should be required for users who need access to multiple computer workstations simultaneously.

16. COMPUTER ROOM LOCATION

Criteria:

- Risk exposure to systems is significantly reduced when the main computer room of an organization is located away from the organization's main office.

Condition:

- The City's main computer room is in City Hall. The majority of the City's systems are located in this room.
- Considering City Hall is a public building and could be a target for vandalism or terrorism, the City's systems are at risk.

Cause:

- Significant funds may be required to relocate the computer room to a non-public building.

Effect:

- Risk of loss of system hardware and data.

Recommendation:

1. IT Management should evaluate and document options available and costs required to relocate the computer room to a non-public building. In conjunction with this analysis, IT Management should evaluate electronic archiving (writing of system data simultaneously to duplicate hard drives in order to protect against loss of data in the event of device failure) to a remote location.

17. EMPLOYEE TERMINATION PROCEDURES

Criteria:

- Procedures addressing measures that must be taken in the case of voluntary and involuntary employee terminations help ensure security to computer system operations and system hardware, software, and data. Procedures of this nature are particularly important when the termination involves IT personnel or an involuntary termination.

Condition:

- While specific procedures are followed by IT when an employee terminates, no written procedures exist outlining procedures IT personnel must take in the case of a voluntary or involuntary employee termination.

Cause:

- IT Management has not documented termination procedures.

Effect:

- Potential security risk to city systems including hardware, software, and data.

Recommendation:

1. IT should develop and document formal termination procedures to be followed by IT personnel.

MANAGEMENT RESPONSES TO AUDIT OF INFORMATION TECHNOLOGY SECURITY

1. RISK ANALYSIS

RECOMMENDATION 1

Management Plan of Action: IT Management agrees that the review of the Risk Analysis should be a formal process. IT will replace the existing signature blocks with a certification of review by the IT Director and the IT Director will confirm his review by placing his signature on the review. Action items will be noted.

Timetable: May 2002

RECOMMENDATION 2

Management Plan of Action: Once the IT Director has certified his review of the Risk Analysis and the Board of Managers has formulated necessary actions, IT will forward the document to the City Manager's Office for further review. IT will solicit comments from CMO.

Timetable: June 2002

RECOMMENDATION 3

Management Plan of Action: IT will establish a baseline for this document and record revisions to the document, to include adds/changes/deletions, date, and author.

Timetable: June 2002

2. INFORMATION TECHNOLOGY SECURITY TRAINING

RECOMMENDATION 1

Management Plan of Action: IT discussion with HR and attendees of the HR Employee Orientation Course revealed that computer security was discussed at this course, though not in depth. The IT Security and Contingency Administrator received verbal agreement with HR to include a larger discussion in the orientation session and to provide a handout on computer security to all course attendees. IT has developed both a short briefing and a handout. HR has also agreed to hand out information security information during the biennial Workplace Violence training sessions. IT will also increase the amount of information available on the intranet's security web pages. The first briefing occurred April 1, 2002. The briefings are scheduled to be repeated the first Monday of every month. Samples of the briefing and handout are included in this package.

Timetable: Pamphlets and HR briefing: June 2002

Web page updates: July 2002

3. INCIDENT AND INTRUSION MONITORING, DETECTION, HANDLING, REPORTING, AND LOGGING

Management remarks: The audit suggests several conditions for this finding with which IT will further clarify. The audit also suggests "...logs are not maintained because of lack of disk space..." IT maintains the logs on-line for approximately 90 days, then the logs are archived and maintained in off-site storage for an additional 90 days.

RECOMMENDATION 1

Management Plan of Action: IT system administrators and the ISCA receive e-mail bulletins from various sources and subscription services that keep them apprised of potential security incidents. The ISCA also reviews information from numerous security websites on a continuous basis. IT does agree that the incident handling process is not formally documented and will:

- * formalize the incident handling process that is currently in use;
- * develop responsibilities and procedures for incident response;
- * will consider the practicality and need for the implementation of a response team.
- * review the current process as it is developing formal documentation and provide published procedures for clients to follow in reporting possible intrusion incidents

Timetable: March 2003

RECOMMENDATION 2

Management Plan of Action: The audit reports that "No system auditing/monitoring tools are in use". In actuality, the NT/Win2K, UNIX, and Unisys have the equivalent to security, application, and event logs enabled and capturing data. Additionally the various business applications have audit logs and audit trails in use. The auditor may have been referring to reporting tools that help sort and sift through the multitude of logs and help alert staff to serious events. IT has reviewed and weighed the value of several solutions, such as CA/Unicenter, but found the cost to be prohibitive (>\$200K). Recently, a flyer for a new tool, designed to aid in monitoring and reporting NT/Win2K logs was received by IT and is currently under review. As reported in a previous audit, IT intends to train and use the Computer Systems Technicians to augment the Systems Administration Specialists in systems monitoring. Prerequisite to that, however, is sufficient training for the Computer systems technicians, and the allowance of sufficient systems privileges to perform the task. IT will formalize monitoring tasks and procedures, while continuing the technician training, evaluating tools, and weighing access requirements. Monitoring tools will be purchased as budget funds are available.

Timetable: Process formalization – August 2002
Personnel training/access – March 2003
Tools evaluation/purchase – November 2002

4. PENETRATION TESTING

RECOMMENDATION 1

Management Plan of Action: During the course of the audit, IT provided the auditors the then existing plans to engage a 3rd party security firm to perform an intrusion test of the City's network and servers. The agreement was processed through City Attorney and forwarded back to IT on February 14. The finalization of the purchasing process will be completed within the next few weeks and the engagement scheduled

Timetable: May 2002

5. SOCIAL ENGINEERING

RECOMMENDATION 1

Management Plan of Action: The specific test that led to this recommendation, entailed elements that confused the responding parties. IT performs validation of a person's identify through several methods. An e-mail message is considered to be sent by the e-mail account holder and therefore is identification, visual recognition of the individual, and voice recognition. Also, certain agencies within the management and elected elements of the City are assumed to have certain elevated levels of authority. In the password-reset scenario described, a member of the Audit Office identified himself, and was recognized by the Help Desk through voice. It was understood that the City Auditors Office authority grants them access to all city information without prior approval. This resulted in the Help Desk resetting a password when it should not have. Under other conditions, the results would have been quite different. Nonetheless, IT will review and modify its procedures and authorization requirement to reduce this vulnerability. The use of Social Security numbers is not viable in light of the need to safeguard such information, and IT does not currently have access to or a list of current supervisors for each employee. When in doubt we will request a manager approval before granting a new password.

Timetable: June 2002

RECOMMENDATION 2

Management Plan of Action: IT will review our existing procedures to address password resetting authorization methods.

Timetable: June 2002

RECOMMENDATION 3

Management Plan of Action: From an operation perspective, following this recommendation would be counterproductive for only minimal security gain. Lockout of password after three invalid attempts was considered by IT, but would place an inordinate burden on existing support staff. The city has several 24x7 operations, including Detention, Fire Services, Public Works, and other agencies, such as Municipal Court and Leisure Services, operate extended and weekend hours. With systems and support staffing available to support only a 5x9 schedule, clients who inadvertently lock out their accounts will have to wait for the next normal work period to regain computer access. The 15-minute delay prevents continuous password tries by hackers but provides a fail-safe for the authorized users during non-standard work hours.

Timetable: N/A - Closed

6. PATCHES

Management Remarks: The audit suggests that there are no patch processes in place thereby placing the infrastructure at risk. In fact, there are processes employed by IT to evaluate and deploy security patches, and functional need patches. The System Administration Specialists subscribe to several monitoring services that alert them to security concerns. Additionally, IT subscribes to vendor mechanisms for patch notification and risk assessment. These patches are applied if they are designated a security risk. Functional patches are evaluated by the user community and applied thru a change control process.

RECOMMENDATION 1

Management Plan of Action: Management agrees that the processes being exercised should be formally documented as policies/procedure. It will execute this task.

Timetable: Completion of formal policies/procedures as applicable by May 2002.

7. WIRELESS SECURITY

Management Remarks: The audit states that four access points were in operation at the time of the audit. In fact only two were in operation, one of which was shut down. The other access points were planned to be activated after pilot study of the 802.1x security

protocol was completed.

RECOMMENDATION 1

Management Plan of Action: IT holds security as a primary consideration in all of its computing and network environments. It is this reason that we do not implement WEP and MAC as enhanced security. WEP encryption keys have been broken by hackers in the past few months and are not considered secure any longer. MAC, which is a hardware identification address, is also vulnerable to detection and cloning, rendering it useless as a security measure. IT has implemented 802.1X which encompasses a per session version of WEP instead of the static WEP. The per session version changes the key for every connection session, vastly increasing the security protection, since, even if a session key is broken, it won't be usable in the next session.

Timetable: N/A – a viable, alternate solution has already been implemented

RECOMMENDATION 2

Management Plan of Action: The access needed by the wireless clients extends beyond the facilities that would be available within our DMZ. The city's wireless solution is supposed to provide the same access as an authenticated client would have if physically wired to the network. Funneling the wireless protocol would require opening additional ports in the firewall to access some of this information and present a greater overall security risk. The wireless clients, with the more robust 802.1X protocol stack, authenticated by the internal Windows client security system have sufficient safeguards to minimize the risk of unauthorized access. IT has no current plans to provide wireless access to anyone other than city employees.

Timetable: N/A -- Closed

RECOMMENDATION 3

Management Plan of Action: Production network equipment is normally secured and administration is controlled via software, hardware or facility security controls. In the future, initial installations of network components will have access protection immediately implemented.

Timetable: Immediately

8. SYSTEM ACCESS AND AUTHENTICATION

RECOMMENDATION 1

Management Plan of Action: On December 20, 2001, IT implemented password hardening for initial log in to the network. The hardening protocol includes alpha, numeric, capital and small letters and special characters.

Timetable: N/A -- Closed

RECOMMENDATION 2

Management Plan of Action: IT runs password-cracking software periodically to analyze the passwords being used by individuals. This program was last run in November and users with insufficient passwords received e-mails requesting they change their password. With the implementation of password hardening, risk of password penetration is greatly reduced. IT will continue to run this program periodically, at least once per quarter.

Timetable: N/A -- Closed

RECOMMENDATION 3

Management Plan of Action: Password change is required every 90 days for all applications. Some commercial applications have no mechanism to require the passwords be changed but every application with that mechanism has the process activated and users have been advised numerous times to change their passwords at least every 90 days. We are unable to modify vendor software, but will request this enhancement from the software vendor. Password security protocols are included as part of the continual security education process IT is implementing.

Timetable: See Security Training Recommendation.

RECOMMENDATION 4

Management Plan of Action: Biometric technology is continually being evaluated by the ISCA. The ISCA conducted a test of proximity badge readers in October 1998, evaluated AirID from RFIdeas in December of 2000 and reviewed Iris scanning technology from Laser Barcode Solutions in November of 2000. All of these biometric solutions were very expensive (approximately 90 to 150 dollars per system) and most were not compatible with all of the applications and platforms currently being used in the city. If a biometric solution was implemented that was not useable across the enterprise and still required application logons, it would be an added burden that would increase administrative overhead without gaining enough additional security to be cost effective.

Timetable: Continual. IT will evaluate the state of the technology continually. IT sees biometrics as a conceptual answer to many of the system access issues to date.

RECOMMENDATION 5

Management Plan of Action: Changing RAS phone numbers would be an administrative burden which would have negative impacts on the user community with little to no gain in security. The audit team has suggested this in previous audits (1999-2002). IT's reasons for not acting on this recommendation is as follows: War dialing software products are readily available that could glean any dial in numbers in a matter of minutes. That is why our current RAS connectivity process requires authentication.

Timetable: N/A -- Closed

RECOMMENDATION 6

Management Plan of Action: Access restrictions based on hours worked would be an administrative burden and would hamper anyone from working outside of their predefined work hours. Since City Departments work 24 by 7 and systems and applications must be available 365 days per year, access restrictions would not significantly increase overall security.

Timetable: N/A -- Closed

9. DOMAIN ADMINISTRATOR RIGHTS

RECOMMENDATION 1

Management Plan of Action: Before access was given to the Computer Systems Technician and the Microcomputer Support Supervisor, IT looked at the security ramifications of this decision. At the time both individuals needed Domain Administrator access to complete some of their work and to meet the needs of the City. It has always been the IT department's policy to provide administrator rights to only the staff that require those rights. Having only 5 people with administrative rights with the number of servers in place and with a total the staff of approximately 100 does not seem to be too many people with this authority. IT will review the current processes and make appropriate changes. The ADMINISTRATOR account is restricted to only three Systems Administration Specialists.

Timetable: Re-evaluation targeted for completion June 30, 2002.

10. ROOT ACCESS

RECOMMENDATION 1

Management Plan of Action: IT has evaluated the need for appropriate access numerous times and has made adjustments when deemed necessary. IT has documented a ROOT ACCESS policy and will provide copies to the CAO. IT will continue to review UNIX root access as third-party products improve, and will make changes if possible.

Timetable: Continual. Next evaluation targeted for June 30, 2002.

RECOMMENDATION 2

Management Plan of Action: The root password is currently being changed every 6 months. IT will change the frequency to every 90 days. As with other processes, IT will formally document this process as well.

Timetable: Immediately

11. LOCAL ADMINISTRATOR

RECOMMENDATION 1

Management Plan of Action: Local administrator accounts provide an individual access only to machines they have physical access to. They do not provide any capability to threaten the network or applications used by that system. IT will continually remind the user community that they should not store any files locally and that any sensitive information should be placed on a secure network drive or a diskette. IT will also rename the administrator account as recommended.

Timetable: Approximately March 1, 2005 for account rename all local administrator accounts.

RECOMMENDATION 2

Management Plan of Action: To change every local administrator accounts would require Microcomputer Support to manage and maintain 1800 different names and passwords. The changing of these accounts and passwords and their maintenance would be an extreme burden to support staff and would add little to security. However, IT will further investigate the use of existing Biometric technologies to better secure these accounts.

Timetable: June 30, 2002 for Biometric evaluation.

12. CONTROL OF COMPUTERS AND EQUIPMENT

RECOMMENDATION 1

Management Plan of Action: IT completes periodic inventories of all resources and works closely with Departments on lost and damaged equipment. In addition to the Support Division inventory process every Department must revalidate the equipment in their areas annually as part of the mandated budget process. Also during the Capital budget and replacement process inventory is looked at continually. And finally with use of the SMS software package every machine is accessed whenever an update must be made to citywide applications.

Timetable: N/A -- Closed

RECOMMENDATION 2

Management Plan of Action: It has inventory procedures in place for all resources. IT will provide the CAO with copies of the procedures.

Timetable: Immediately.

RECOMMENDATION 3

Management Plan of Action: The current "Use" document details the employee responsibility in the care of resources. Repercussions for misuse are left to individual Department management and can include employee-required replacement of lost inventory. HR also has a policy on the misuse of any City resource. Abuse of any city owned property should require appropriate penalties.

Timetable: N/A -- Closed

RECOMMENDATION 4

Management Plan of Action: IT defers enforcement for abuse of resources to each Department. Loss has been minimal over the past few years. IT does charge Departments for replacement of some resources but it is left up to the Department to determine penalties for individual users. The IT department would not want to dictate to Departments the penalties they enforce on their employees.

Timetable: N/A -- Closed

13. LONG DISTANCE CODES

RECOMMENDATION 1

Management Plan of Action: IT agrees with the auditor on code activation. The Support Division will work with the carrier to ensure unused Long distance codes are

inactive. We will activate codes in blocks of 100 and issue only upon valid request.

Timetable: Completed and implemented February 2002.

RECOMMENDATION 2

Management Plan of Action: IT changed the codes from 4 to 5 based on a previous audit finding. Another change at this time would be a burden for both IT and the user community. It is felt that changing the codes from 5 to 6 characters would not significantly increase security. Additional, since long distance charges are required to be reconciled monthly, inappropriate use is quickly addressed.

Timetable: N/A -- Closed

RECOMMENDATION 3

Management Plan of Action: Changing long distance codes on a regular basis would require coordination with our long distance carrier and results in charges to the city (\$20 per change request). The administrative burden and cost **does not warrant the benefit.**

Timetable: N/A -- Closed

14. SECURITY COMMITTEE

RECOMMENDATION 1

Management Plan of Action: The Security Committee has a clearly defined charter that was provided to both Departmental sponsors and provided to senior management. The charter defines the role of the committee, which includes all areas of security. The committee is an advisory board for all security concerns and IT issues are brought to the committee when deemed necessary. The ISCA keeps the group apprised of all IT security related changes. IT agrees that the charter, roles and responsibilities need more broad recognition and will pursue that objective.

Timetable: Immediately

RECOMMENDATION 2

Management Plan of Action: The IT Board of Managers, the Configuration Control Committee and the ISCA work closely together to review all IT security related changes. It would not be beneficial to create another committee just to address IT Security.

Timetable: N/A -- Closed

15. MULTIPLE SESSIONS

RECOMMENDATION 1

Management Plan of Action: Providing employees the capability of having multiple active sessions is extremely important in many departments. With the current mobile workforce limiting sessions or assigning users to particular workstations is impractical. Additionally, many departments with counter operations change employees frequently and the changes are of a short duration. Requiring a person to log off of their existing session before logging into a second session interrupts their current activities and provides little if any additional security. In addition to counter operations, IT personnel doing fieldwork, persons attending training and persons using laptops for meetings would be negatively impacted by a change of this nature. IT agrees to enforce system lockouts upon non-activity of 15-minute intervals.

Timetable: March 2002

16. COMPUTER ROOM LOCATION

RECOMMENDATION 1

Management Plan of Action: IT agrees that having the computer room in a public facility is not an ideal situation. IT has looked several times over the years at relocating the computer room but it has always been considered cost prohibitive. Over the last several months, IT looked at the cost effectiveness of leasing or purchasing a facility on the southeast side of town. The cost to lease was \$18,000 per month and the purchase price was \$2,000,000. In addition to the cost of the facility IT also estimated a cost of \$1,700,000 in telecommunications costs to move the Computer Room to the proposed location. With the current curtailed budget in the City, IT does not consider relocation practical at this time.

The second part of the recommendation concerns Disk Mirroring. This technology is extremely expensive for the amount of disk space used in the City and has not been considered because the user community, through the Contingency Task Force, has stated that systems can be unavailable for one business day and that one day's work can be manually recovered. All applications are backed up daily and loss of all systems would result in, at most, a one-day loss of electronic data. Given that this recommendation was actually addressing automated archiving of mission-critical data, IT will evaluate usage for applicability and ROI.

Timetable: March 2003

17. EMPLOYEE TERMINATION PROCEDURES

RECOMMENDATION 1

Management Plan of Action: HR provides IT with up-to-date information on all employee terminations. The ISCA provides that information to appropriate personnel. A procedure already exists for the actions taken by the ISCA. The actions include contacting appropriate personnel to remove accesses from individuals when the ISCA is notified, via e-mail, from HR. The ISCA also completes a secondary follow up when the Oracle alert is sent from the HR Application. IT will review all processes in the chain to ensure they are all appropriately documented.

Timetable: May 31, 2002.